UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

UNITED STATES OF AMERICA	*	
v.	*	**Criminal No. GJH-19-0096**
CHRISTOPHER PAUL HASSON	*	

* * * * * * * * * * *

MOTION TO SUPPRESS EVIDENCE SEIZED PURSUANT TO SEARCH WARRANTS

Defendant Christopher Hasson, through undersigned counsel, hereby moves this Honorable Court to suppress evidence seized pursuant to search warrants dated January 11, 2019, as well as all derivative evidence, including evidence seized pursuant to subsequent search warrants, on the ground that those warrants failed to establish probable cause.

I. PROCEDURAL BACKGROUND

A. January 11th Search Warrants

On January 11, 2019, FBI Agent Rachid Harrison submitted an affidavit to Magistrate Judge Charles Day seeking warrants to (1) place a GPS tracker on Mr. Hasson's car, (2) seize and search the contents of two of Mr. Hasson's private email accounts, and (3) obtain historical cell-site location information for Mr. Hasson's cell phone. *See* January 11, 2019 Application, attached as Exhibit A, at 2-3. The affidavit also sought a prospective order directing Mr. Hasson's cell provider to hand over information regarding communications to or from his phone for 45 days following the date of the order. Ex. A at 37. Agent Harrison asserted he had probable cause to believe the warrants would produce evidence of violations of 18 U.S.C. §§ 1111 (murder in federal jurisdiction), 1114 (murder or attempted murder of officers or employees of the United States), 351 (assassination of Cabinet secretaries,

members of Congress, or Supreme Court justices), and 371 (conspiracy to commit the foregoing crimes). Ex. A at 3-4.

The affidavit alleges that Mr. Hasson, a lieutenant in the U.S. Coast Guard, holds a number of "Extremist Views" and is a "White Nationalist" who "advocates for 'focused violence' in order to establish a white homeland." Ex. A at 6. According to the affidavit, Mr. Hasson used his Coast Guard computer to research and plan for possible violent attacks against U.S. senators, Supreme Court justices, political commentators, and others. Ex. A at 6, 12-13. Specifically, Mr. Hasson, while at work, allegedly visited websites selling firearms and tactical gear; reviewed various portions of a manifesto written by Anders Behring Breivik, a Norwegian "far-right domestic terrorist" who killed 77 people in 2011; performed internet searches on where certain government officials live and whether they receive Secret Service protection; searched for rental cars he could use during an attack; and read up on explosive substances such as "Smokeless Powder" and nitroglycerine, among other things. Ex. A at 7, 9-10, 13, 18-20.

The affidavit also alleges Mr. Hasson sent various documents back and forth between his work email account and two different personal email accounts, referred to in the affidavit as TARGET EMAIL-1 and TARGET EMAIL-2. Ex. A at 3. Among the alleged communications are the following:

- On March 26, 2017, Mr. Hasson sent Breivik's 1,518-page manifesto from TARGET EMAIL-1 to his work account. Ex. A at 8.
- On May 18, 2017, Mr. Hasson sent the memoirs of two convicted domestic terrorists, Eric Rudolph and Ted Kaczynski, from TARGET EMAIL-1 to his work account. Ex. A at 8, 20-21.

- On May 25, 2017, Mr. Hasson sent a map of Shenandoah National Park from TARGET EMAIL-1 to his work account. Ex. A at 21.
- On May 30, 2017, Mr. Hasson sent a document called "Imagining the Impossible: Insurgency in the U.S.A." from TARGET EMAIL-1 to his work account. Ex. A at 21.
- On June 2, 2017, Mr. Hasson used TARGET EMAIL-1 to send to his work account a link related to "energetic materials," i.e., bomb-making. Ex. A at 21.
- On June 5, 2017, Mr. Hasson sent a document called "The Saxon Messenger," which contains anti-Semitic propaganda, from TARGET EMAIL-1 to his work account. Ex. A at 21.
- On June 7, 2017, Mr. Hasson used TARGET EMAIL-1 to send a number of documents to his work account, including "The Terrorist's Handbook," "Anarchist Cookbook," "Improvised Munitions Handbook (Improvised Explosive Devices or IEDs)," "Emailing Anon – How to make Semtex," and "Home Workshop Explosives." Ex. A at 21-22.
- On July 10, 2017, Mr. Hasson used TARGET EMAIL-1 to send to his work account a link for Navy Seal ballistic plate carriers from London Bridge Trading Company. Ex. A at 22.
- On September 29, 2017, Mr. Hasson used TARGET EMAIL-1 to send to his work account a letter in which he describes himself as a white nationalist. Ex. A at 6-7.

- On March 24 and November 30, 2017, Mr. Hasson sent photographs of "assault-style rifles" to his work email account from TARGET EMAIL-1 and TARGET EMAIL-2, respectively. Ex. A at 10.
- On February 15, 2018, Mr. Hasson sent a link for "The young Hitler I Knew" from his work account to TARGET EMAIL-1. Ex. A at 22.
- On February 22, 2018, Mr. Hasson sent a ballistics report for a .308 rifle from his work email account to TARGET EMAIL-1. Ex. A at 22.
- On March 5, 2018, Mr. Hasson sent a document called "Mathematics for Precision Shooter" from his work email account to TARGET EMAIL-1. Ex. A at 22.
- On August 21, 2018, Mr. Hasson used his work email account to review emails he had sent from TARGET EMAIL-1, which contained documents titled "The Saxon Messenger," "Improvised Munitions Handbook (Improvised Explosive Devices or IEDs)," and "Between the Lines of Drift" (Eric Rudolph's manifesto). Ex. A at 22-23.
- On November 13, 2018, Mr. Hasson used his work email account to send to TARGET EMAIL-1 a link to a website for "The Center for Syncretic Studies," a neo-fascist think tank. Ex. A at 23.
- On November 19, 2018, Mr. Hasson sent a link for a website describing autonomous self-driving tactical vehicles from his work email account to TARGET EMAIL-1. Ex. A at 23.
- On December 11, 2018, Mr. Hasson sent Ted Kaczynski's manifesto from his work email account to TARGET EMAIL-1. Ex. A at 23.

Based on Agent Harrison's affidavit, Judge Day signed four separate search warrants on January 11, 2019.

The first warrant directed Verizon Wireless to disclose certain information relating to Mr. Hasson's cell phone account "for the time period January 1, 2017, through the present." Cell Phone Warrant, attached as Exhibit B, at 4. Among the categories of information are "[a]ll records and other information (not including the contents of communications) relating to wire and electronic communications sent or received by [Mr. Hasson's phone]," including (1) "the date and time of the communication, the method of the communication, and the source and destination of the communication," and (2) "information regarding the cell tower and antenna face (also known as 'sectors') through which the communications were sent and received, as well as per-call measurement data (also known as 'real-time tool' or 'RTT')." Ex. B at 5. The warrant also ordered Verizon to provide similar information about Mr. Hasson's phone "for a period of 45 days from the date of this warrant." Ex. B at 5.

The second warrant directed Oath Holdings, Inc., to hand over (1) "[t]he contents of all emails associated with [TARGET EMAIL-1] from January 1, 2017, through the present," (2) "[a]ll records or other information regarding the identification of the account," (3) "[a]ll records or other information stored by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files," and (4) "[a]ll records pertaining to communications between [Oath Holdings] and any person regarding the account." Target Email-1 Warrant, attached as Exhibit C, at 4-5. The third warrant ordered Google to furnish similar information about TARGET EMAIL-2, but only for the period "from November 1, 2017, through December 31, 2017." Target Email-2 Warrant, attached as Exhibit D, at 4-5.

Finally, the fourth warrant instructed police to install a tracking device on Mr. Hasson's Subaru in order to monitor the car's location for 45 days. GPS Warrant, attached as Exhibit E, at 1.

B. January 22nd Search Warrants

On January 22, 2019, Agent Harrison submitted to Magistrate Judge Timothy Sullivan an application seeking a warrant for email records during an expanded window of time. Specifically, the application sought (1) TARGET EMAIL-1 records from January 1, 2016, to December 31, 2016, and from January 11, 2019, to the present, as well as (2) TARGET EMAIL-2 records "for the entire time frame from January 1, 2016, through the present." January 22, 2019 Application, attached as Exhibit F, at 5. The application asserted probable cause to believe these records would contain evidence of violations of the statutes identified in the January 11th application, as well as 21 U.S.C. § 844 (simple possession of Tramadol, a Schedule IV controlled substance), 21 U.S.C. § 952 (importation of Tramadol), and 18 U.S.C. § 922(g)(3) (possession of a firearm by an unlawful user of a controlled substance). Ex. F at 3.

Agent Harrison's affidavit relied on evidence discovered through execution of the January 11th warrants, in addition to information contained in the affidavit supporting those warrants. *See, e.g.*, Ex. F at 16-17 (discussing "records obtained for TARGET EMAIL-2" and "emails recovered from a prior search of TARGET EMAIL-1"), 32-38 (similar). Judge Sullivan signed the warrants later on the 22nd. Second Target Email-1 Warrant, attached as Exhibit G, at 1; Second Target Email-2 Warrant, attached as Exhibit H, at 1.

C. February 8th Search Warrants

On February 8, 2019, FBI Special Agent Alexandria Marie Thoman submitted an application seeking a warrant for TARGET EMAIL-1 and TARGET EMAIL-2 records for

the period since execution of the January 22nd warrants. February 8, 2019 Application and Warrant, attached as Exhibit I, at 4. Agent Thoman claimed she had probable cause to believe the search would turn up evidence of violations of the statutes enumerated in January 22nd application.

To establish probable cause, the application cited to evidence from execution of the two previous rounds of warrants. *See, e.g.*, Ex. I at 11, 15-17, 35-40 (referencing information found during "a prior search warrant of TARGET EMAIL-1" and "evidence from the original search warrant of TARGET EMAIL-2"). Judge Thomas DiGirolamo signed the warrants on February 8th. Ex. I at 60-64.

D. February 12th Search Warrant

On February 12, 2019, Special Agent Erik Hayes of the Coast Guard Investigative Service submitted a warrant application to a military judge. February 12, 2019 Application, attached as Exhibit J. Agent Hayes wrote that "[r]eviews of personal email accounts belonging to LT Hasson, pursuant to Federal search warrants for items pertaining to acts associated with domestic terrorism, revealed indicators of the purchase and use of controlled substances." Ex. J at 3. Follow-up warrants allegedly "revealed LT Hasson frequently purchases Tramadol, a Schedule IV controlled substances, from a supplier in Mexico." Ex. J at 3. Agent Hayes explained that Tramadol requires a valid prescription, which Coast Guard medical records indicated Mr. Hasson did not have. Ex. J at 3. In addition, "[v]ideo surveillance" of Mr. Hasson's cubicle supposedly showed him "consuming an unknown substance in pill form on a daily basis." Ex. J at 3.

Based on these allegations, Agent Hayes sought a warrant to search "the assigned personal workspace of LT Hasson" at Coast Guard headquarters. Ex. J at 4. Agent Hayes asserted he had probable cause to believe such a search would produce evidence of violations

of Article 112a, U.C.M.J. (wrongful use or possession of a controlled substance), 21 U.S.C. § 844 (simple possession of Tramadol, a Schedule IV controlled substance), and 21 U.S.C. § 952 (importation of Tramadol). Ex. J at 3. The military judge signed the warrant later on the 12th. Ex. J at 6.

E. February 14th Search Warrants

On February 14, 2019, Agent Thoman submitted a warrant application to Magistrate Judge Gina Simms, seeking authorization to search Mr. Hasson's apartment, his car, and two additional private email accounts (TARGET EMAIL-5 and TARGET EMAIL-6), as well as to draw and test his blood for Tramadol. February 14, 2019 Application, attached as Exhibit K, at 2-3. This search, Agent Thoman averred, would turn up evidence of the homicide, firearm, and controlled substance offenses identified in previous warrant applications. Ex. K at 3.

The application explained that "[a]gents have obtained records pursuant to [prior] email warrants and have conducted an initial review; certain information from emails obtained from those warrants is included in this affidavit." Ex. K at 5. The portion of the application attempting to establish probable cause for firearm offenses, in particular, relied on evidence recovered during execution of previous warrants. Agent Thoman's assertion that Mr. Hasson "appears to have actually acquired firearms, firearms equipment, and ammunition" is supported by numerous citations to, for example, "emails obtained from a search of TARGET EMAIL-1" and "records obtained for TARGET EMAIL-2." Ex. K at 12; *see also, e.g.*, Ex. K at 13 ("certain emails obtained from TARGET EMAIL-1" and "an email obtained from TARGET EMAIL-1"), 14 ("records from the search warrants for TARGET EMAIL-1"), 15 ("[r]ecords from a prior search of TARGET EMAIL-1"), 16 ("[r]ecords from

a prior search warrant of TARGET EMAIL-1"), 17 ("[r]ecords obtained from a prior search of TARGET EMAIL-1"), 18 ("an email from TARGET EMAIL-1").

Likewise, the application's supposed probable cause for the controlled substance offenses relied on information recovered pursuant to previous warrants. *See, e.g.*, Ex. K at 25 ("Using TARGET EMAIL-1, TARGET EMAIL-5, and TARGET EMAIL-6, HASSON placed orders by sending emails to his supplier at TARGET EMAIL-3."), 26 ("The chart below summarizes records from prior email search warrants for TARGET EMAIL-1 and TARGET EMAIL-3, and information obtained by subpoenas to UPS, FedEx, MoneyGram, and Western Union."), 27 (citing "emails obtained from TARGET EMAIL-1"), 28 (same), 30 (same), 31 ("[O]n February 14, 2017, using TARGET EMAIL-1, HASSON sent two emails to TARGET EMAIL-6.").

Judge Simms signed the warrants later on the 14th. February 14th Warrants, attached as Exhibit L.

II. ARGUMENT

A. Evidence Seized Pursuant to the January 11th Search Warrants Is Inadmissible.

"As a general rule, the Fourth Amendment requires that law enforcement searches be accompanied by a warrant based on probable cause." *United States v. Kolsuz*, 890 F.3d 133, 137 (4th Cir. 2018). A warrant is supported by probable cause if the facts alleged in the affidavit establish "a fair probability that contraband or evidence of a crime will be found in a particular place." *United States v. Lyles*, 910 F.3d 787, 791 (4th Cir. 2018). "Probable cause only exists when an officer has a reasonable belief that a law has been broken," and an "officer cannot have a reasonable belief that a violation of the law occurred when the acts to which an officer points as supporting probable cause are not prohibited by

law." *United States v. Williams*, 740 F.3d 308, 312 (4th Cir. 2014); *see also Doe v. Broderick*, 225 F.3d 440, 452 (4th Cir. 2000) ("[A] mere hunch that illegal activity is afoot will not provide a valid foundation for the issuance of a search warrant.").

Here, Agent Harrison's application for the January 11th warrant does not establish a "fair probability" that Mr. Hasson's email accounts, his historical cell-site data, or the movements of his car will contain evidence of murder, assassination, or conspiracy to commit those offenses. The application alleges that Mr. Hasson holds "extremist views" and supports that assertion by quoting an email in which he describes himself as a "white nationalist." Ex. A at 6. It also describes in detail Breivik's "far-right" views—including his disdain for "Cultural Marxism" and his fear of the "islamization of Europe"—and alleges Mr. Hasson read portions of Breivik's manifesto. Ex. A at 7-9, 12, 15-20. But endorsing extreme or unpopular opinions is not a crime, and it cannot form the basis to believe Mr. Hasson had committed murder or assassination. *See Ostergren v. Cuccinelli*, 615 F.3d 263, 270-71 (4th Cir. 2010) ("The First Amendment means that government has no power to restrict expression because of its message, its ideas, its subject matter, or its content.").

Agent Harrison's application also alleges Mr. Hasson visited websites that sold firearms; emailed himself pictures of guns and tactical gear; received shipments from companies that sell (among other things) guns and ammunition; created a spreadsheet listing "weapons, survival gear, and provisions"; researched how to create a disguise; conducted internet searches regarding various government officials and the "protection" they received; Googled "rental cars near me"; read documents that discussed how to create explosive substances; and visited a bomb-making website. Ex. A at 10-11, 13, 18, 20, 21. But none of these alleged actions is "prohibited by law," and thus they do not establish probable cause

to believe that "a law has been broken"—much less one of the laws enumerated in the application. *Williams*, 740 F.3d at 312. Although the application's allegations may suggest Mr. Hasson, at some point, was thinking about these types of activity, entertaining such thoughts is not a crime. Probable cause demands that a law has, in fact, "been broken."[1] *Id.*

Even if allegations of an as-yet-uncommitted crime could give rise to probable cause in some cases, Agent Harrison's application would fall short. That application does not allege Mr. Hasson had conceived of, much less actually begun to plan for, any specific murder. It does not allege, for instance, that Mr. Hasson decided to kill a specific senator, that he selected a site for the murder, that he chose a date on which to commit the crime, or that he took any other concrete steps that might in fact lead to criminal conduct. Instead, the application includes allegations of generalized interest in his political opponents' demise, untethered to any specific plans to achieve that end.

The timeframe of the events described in the application supports this conclusion. The application recounts Mr. Hasson's actions over the course of two years, from January 2017 until January 2019—a lengthy period of time that belies the idea Mr. Hasson was acting with any urgency. Such a plodding pace is more indicative of someone who reads on his

[1] Moreover, Agent Harrison's framing of some of the application's factual allegations misleadingly suggests innocent conduct is in fact indicative of criminal intent. The application notes, for instance, that (1) the Breivik manifesto instructs would-be attackers that they will "have to buy/rent a car" to facilitate their escape, and (2) Mr. Hasson "performed multiple [internet] searches for 'rental cars near me.'" Ex. A at 18. According to the application, the latter fact indicates Mr. Hasson "conducted internet searches consistent with Breivik's instruction." Ex. A at 18. But Mr. Hasson performed the relevant searches in July 2017—a year and a half *before* he read the portion of Breivik's manifesto that discusses rental cars. Ex. A at 18. Thus Mr. Hasson's search for a rental car does nothing to suggest he was following Breivik's instructions or plotting an attack of the kind Breivik carried out.

computer to dispel his boredom at work than of someone with imminent plans to engage in criminal conduct.

Nor does the application demonstrate probable cause by including two inchoate crimes—attempted murder of a federal employee (18 U.S.C. § 1114) and conspiracy to commit murder or assassination (18 U.S.C. § 371)—among the offenses for which Agent Harrison hoped to search for evidence. *See* Ex. A at 3-4.

First, the conduct alleged in the application does not add up to an attempt to commit murder. "An attempt to commit a crime, which is recognized as a crime distinct from the crime intended by the attempt, punishes conduct that puts in motion events that would, from the defendant's point of view, result in the commission of a crime but for some intervening circumstance." *United States v. Pratt*, 351 F.3d 131, 135 (4th Cir. 2003). To convict a defendant of attempt, the government must show he took a "substantial step" toward commission of a substantive offense. *United States v. Sterling*, 860 F.3d 233, 242 (4th Cir. 2017). A "substantial step is a direct act in a course of conduct planned to culminate in commission of a crime that is strongly corroborative of the defendant's criminal purpose. It is more than mere preparation but less . . . than completion of the crime." *United States v. Engle*, 676 F.3d 405, 423 (4th Cir. 2012) (ellipsis in original).

The allegations in Agent Harrison's application are insufficient even to establish that Mr. Hasson engaged in "preparation" to commit a crime: he read several manifestos, ran a number of Google searches, and prepared an Excel spreadsheet. *Id.* There is no allegation that he did anything other than sit behind his computer and use the internet. If Agent Harrison had alleged Mr. Harrison scoped out potential victims' homes in person or visited a shooting range to practice his marksmanship, the application might cross the threshold

between "mere preparation" and a "substantial step." But as it is, the application contains no facts that are "*strongly* corroborative of [Mr. Hasson's] criminal purpose." *Id.* (emphasis added).

Second, Agent Harrison's application also fails to allege facts amounting to a conspiracy. Conspiracy under § 371 "has three elements: an unlawful agreement to commit an offense, the defendant's knowing and willing participation, and an overt act in furtherance of the conspiracy." *United States v. Camara*, 908 F.3d 41, 46 (4th Cir. 2018). To satisfy the first element, the government must prove "an agreement between *two or more people*." *Id.* (emphasis added). Nowhere does Agent Harrison allege, however, that Mr. Hasson has formed an agreement with another person to commit the substantive offenses listed in the application (murder in federal jurisdiction, murder of federal officers, and assassination of high-level government officials). Without such an agreement, there can be no conspiracy; agreement with another is not the same thing as planning on one's own. It is telling, in this regard, that the government has not charged Mr. Hasson with conspiracy (or attempt) to commit murder—presumably because it knows it lacks sufficient evidence.

Finally, even if Agent Harrison's application contained sufficient facts, it would fail to establish probable for another reason: those facts are stale. "[T]here is no question that time is a crucial element of probable cause." *United States v. Richardson*, 607 F.3d 357, 370 (4th Cir. 2010). As a result, a "search warrant may issue only upon allegations of facts so closely related to the time of the issue of the warrant as to justify a finding of probable cause *at that time*." *United States v. Doyle*, 650 F.3d 460, 474 (4th Cir. 2011) (emphasis in original). Thus "evidence seized pursuant to a warrant supported by 'stale' probable cause

is not admissible in a criminal trial to establish the defendant's guilt." *Richardson*, 607 F.3d at 369.

The "vitality of probable cause cannot be quantified by simply counting the number of days between the occurrence of the facts supplied and the issuance of the affidavit." *United States v. Farmer*, 370 F.3d 435, 439 (4th Cir. 2004). "Rather, [courts] must look to all the facts and circumstances of the case, including the nature of the unlawful activity alleged, the length of the activity, and the nature of the property to be seized." *Id.*

Here, Agent Harrison's application relies predominantly on events occurring well before he submitted the application to Judge Day. Most of the emails that Mr. Hasson allegedly sent to or from TARGET EMAIL-1 and TARGET EMAIL-2 were written in the spring and summer of 2017—many months before Judge Day signed the warrants in January 2019. Only three of the many emails described in Agent Harrison's affidavit were sent after August of 2018. *See* Ex. A at 23 (describing emails from November 13, November 19, and December 11, 2018). Thus the large majority of the information in that affidavit was at least five months old—and in many cases, much older than that—at the time Judge Day considered Agent Harrison's application.

The Fourth Circuit has indicated that a similar lag between illegal activity and an application for a warrant does not render the supporting information stale, *as long as* the affidavit alleges the defendant is involved in an "elaborate and ongoing" course of conduct. *See Farmer*, 370 F.3d at 439 (citing six-month delay in *United States v. Leasure*, 319 F.3d 1092, 1099 (9th Cir. 2003)); *see also id.* (holding information not stale where defendant "was under investigation for trafficking in counterfeit clothing and money laundering—not mere isolated violations of the law, but criminal activities of a protracted and continuous nature");

United States v. McCall, 740 F.2d 1331, 1336 (4th Cir. 1984) (explaining that in previous case, Fifth Circuit properly "determined that the ongoing nature of a marijuana-cultivating operation warranted the magistrate's inference that marijuana plants observed in June would still be present in October" (citation omitted)).

But Agent Harrison's affidavit does not allege any such "ongoing" course of conduct. Rather, it simply describes discrete instances of email activity, the large majority of which occurred many months before January 2019, without explaining how those incidents comprise an ongoing offense. Because Agent Harrison failed to include any other evidence of criminal activity involving TARGET EMAIL-1 and TARGET EMAIL-2, his affidavit does not establish probable cause that those email accounts would contain evidence of a crime at the time the January 11th warrants issued. *See Richardson*, 607 F.3d at 370 ("We conclude that a delay of four months does not preclude a finding of probable cause based on staleness *in light of the other information supplied by Agent White* . . . ." (emphasis added)). Nor does it give rise to probable cause to believe Mr. Hasson was then engaged in criminal activity, such that police should be permitted to monitor his movements through historical cell-site data or placement of a location tracker on his car.

All evidence seized pursuant to the January 11th warrants—which were obtained on the basis of stale facts that do not add up to probable cause—is therefore inadmissible. *Richardson*, 607 F.3d at 369; *see also United States v. Terry*, 909 F.3d 716, 721 (4th Cir. 2018) ("In general, evidence discovered as a result of a Fourth Amendment violation is subject to suppression under the exclusionary rule.").

B. Evidence Seized Pursuant to the Subsequent Search Warrants Is Inadmissible.

The exclusionary rule "reaches not only primary evidence obtained as a direct result of an illegal search or seizure, but also evidence later discovered and found to be derivative of an illegality or fruit of the poisonous tree." *United States v. DeQuasie*, 373 F.3d 509, 519 (4th Cir. 2004). Evidence seized pursuant to the January 22nd, February 8th, February 12th, and February 14th warrants is inadmissible under this "derivative evidence" principle.

The affidavits in support of those latter warrants contain much of the same background information that is in the January 11th affidavit. In all the non-military warrant applications, for instance, the affiant describes Mr. Hasson's allegedly extremist views, *see* Ex. A at 6-7, Ex. F at 6-7, Ex. I at 5-7, Ex. K at 7-8; recounts Mr. Hasson's perusal of the Breivik manifesto at work, *see, e.g.*, Ex. A at 12, Ex. F at 18, Ex. I at 18, Ex. K at 18-19; alleges that Mr. Hasson conducted an internet search for the home and work addresses of MSNBC commentator Joe Scarborough, *see* Ex. A at 13, Ex. F at 19, Ex. I at 19, Ex. K at 20; and, except in the February 14th application, lists the messages Mr. Hasson sent among his work email account, TARGET EMAIL-1, and TARGET EMAIL-2, *see* Ex. A at 20-23, Ex. F at 29-32, Ex. I at 31-34, among many other similarities. The passage of a month did not render this information any more probative of the commission of a crime than it had been on January 11th. And indeed, the information had only become staler by the time the follow-up warrants were issued.

Apart from repeating this background information, the follow-up applications rely principally on evidence obtained during execution of the January 11th warrants. Agent Harrison's January 22nd affidavit, for example, repeatedly attempts to establish probable cause by citing to "records obtained for TARGET EMAIL-2," *e.g.*, Ex. F at 16; "emails

recovered from a prior search of TARGET EMAIL-1," *e.g.*, Ex. F at 16; and "records from a prior search warrant of TARGET EMAIL-1," *e.g.*, Ex. F at 17. Agent Thoman's February 8th affidavit does the same, *see, e.g.*, Ex. I at 11 ("records from a prior search warrant of TARGET EMAIL-1"), 12 ("[r]ecords from a prior search of TARGET EMAIL-1"), 14 (same), 35 ("records from prior email search warrants for TARGET EMAIL-1"), as does her February 14th affidavit, *see, e.g.*, Ex. K at 12 ("records obtained for TARGET EMAIL-2"), 13 ("certain emails obtained from TARGET EMAIL-1"), 14 ("records from the search warrants for TARGET EMAIL-1"). And Agent Hayes' application to a military judge also grounds probable cause in evidence found in "personal email accounts belonging to LT Hasson," which were searched "pursuant to Federal search warrants." Ex. J at 3.

As explained above, the records recovered from the January 11th searches of TARGET EMAIL-1 and TARGET EMAIL-2 were obtained illegally. Evidence seized during execution of the January 22nd, February 8th, February 12th, and February 14th warrants—the probable cause for which relied on that "fruit of the poisonous tree"—is therefore "derivative of [the] illegality" underlying the initial warrant. *DeQuasie*, 373 F.3d at 519. As a result, evidence from the latter searches must also be suppressed. *Id.*

III. CONCLUSION

For the reasons described above, this Court should suppress all evidence seized pursuant to the January 11th, January 22nd, February 8th, February 12th, and February 14th search warrants.

Respectfully submitted,

JAMES WYDA
Federal Public Defender

/s/

ELIZABETH G. OYER, #95458
CULLEN MACBETH, #810923
Assistant Federal Public Defenders
100 South Charles Street
Tower II, 9th Floor
Baltimore, Maryland 21201
Telephone: (410) 962-3962
Facsimile: (410) 962-0872
Email: liz_oyer@fd.org
cullen_macbeth@fd.org